

- [12] J. Ménétrey, M. Pasin, P. Felber, and V. Schiavoni, “WebAssembly as a Common Layer for the Cloud-Edge Continuum,” in *Proceedings of the 2nd Workshop on Flexible Resource and Application Management on the Edge*, FRAME ’22, p. 3–8, 2022.
- [13] M. Chadha, N. Krueger, J. John, A. Jindal, M. Gerndt, and S. Benedict, “Exploring the Use of WebAssembly in HPC,” in *Proceedings of the 28th ACM SIGPLAN Annual Symposium on Principles and Practice of Parallel Programming*, PPOPP ’23, p. 92–106, 2023.
- [14] J. Cabrera-Arteaga, M. Monperrus, and B. Baudry, “Scalable Comparison of JavaScript V8 Bytecode Traces,” in *Proceedings of the 11th ACM SIGPLAN International Workshop on Virtual Machines and Intermediate Languages, VMIL at SPLASH 2019*, pp. 22–31, 2019.
- [15] NSA, “National Cyber Leap Year.” [https://www.nitrd.gov/nitrdgroups/index.php?title=National\\_Cyber\\_Leap\\_Year](https://www.nitrd.gov/nitrdgroups/index.php?title=National_Cyber_Leap_Year), 2021.
- [16] G. Goth, “Addressing the Monoculture,” *IEEE Security & Privacy*, vol. 1, no. 06, pp. 8–10, 2003.
- [17] M. N. Hoque and K. A. Harras, “WebAssembly for Edge Computing: Potential and Challenges,” *IEEE Communications Standards Magazine*, vol. 6, no. 4, pp. 68–73, 2022.
- [18] T. Rokicki, C. Maurice, M. Botvinnik, and Y. Oren, “Port Contention Goes Portable: Port Contention Side Channels in Web Browsers,” in *ASIA CCS ’22: ACM Asia Conference on Computer and Communications Security*, pp. 1182–1194, 2022.
- [19] S. Song, S. Park, and D. Kwon, “metaSafer: A Technique to Detect Heap Metadata Corruption in WebAssembly,” *IEEE Access*, vol. 11, pp. 124887–124898, 2023.
- [20] D. Lehmann, J. Kinder, and M. Pradel, “Everything Old is New Again: Binary Security of WebAssembly,” in *29th USENIX Security Symposium*, pp. 217–234, 2020.
- [21] Q. Stiévenart, C. D. Roover, and M. Ghafari, “Security Risks of Porting C Programs to Webassembly,” in *SAC ’22: The 37th ACM/SIGAPP Symposium on Applied Computing*, pp. 1713–1722, 2022.
- [22] D. Genkin, L. Pachmanov, E. Tromer, and Y. Yarom, “Drive-by Key-extraction Cache Attacks from Portable Code,” *IACR Cryptol. ePrint Arch.*, p. 119, 2018.

- [23] G. Maisuradze and C. Rossow, “ret2spec: Speculative Execution Using Return Stack Buffers,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS*, pp. 2109–2122, 2018.
- [24] M. Musch, C. Wressnegger, M. Johns, and K. Rieck, “Thieves in the Browser: Web-based Cryptojacking in the Wild,” in *Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, Canterbury, UK, August 26-29, 2019*, pp. 4:1–4:10, ACM, 2019.
- [25] E. Tekiner, A. Acar, A. S. Uluagac, E. Kirda, and A. A. Selçuk, “In-browser Cryptomining for Good: An Untold Story,” in *IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2021, Online Event, August 23-26, 2021*, pp. 20–29, IEEE, 2021.
- [26] R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, and G. Vigna, “MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS*, pp. 1714–1730, 2018.
- [27] A. Romano, Y. Zheng, and W. Wang, “MinerRay: Semantics-aware Analysis for Ever-evolving Cryptojacking Detection,” in *35th IEEE/ACM International Conference on Automated Software Engineering, ASE 2020, Melbourne, Australia, September 21-25, 2020*, pp. 1129–1140, IEEE, 2020.
- [28] F. N. Naseem, A. Aris, L. Babun, E. Tekiner, and A. S. Uluagac, “MINOS: A Lightweight Real-time Cryptojacking Detection System,” in *28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021*, The Internet Society, 2021.
- [29] W. Wang, B. Ferrell, X. Xu, K. W. Hamlen, and S. Hao, “SEISMIC: SEcure In-lined Script Monitors for Interrupting Cryptojacks,” in *Computer Security - 23rd European Symposium on Research in Computer Security, ESORICS*, vol. 11099, pp. 122–142, 2018.
- [30] J. D. P. Rodriguez and J. Posegga, “RAPID: Resource and API-based Detection Against In-browser Miners,” in *Proceedings of the 34th Annual Computer Security Applications Conference, ACSAC 2018, San Juan, PR, USA, December 03-07, 2018*, pp. 313–326, ACM, 2018.
- [31] A. Kharraz, Z. Ma, P. Murley, C. Lever, J. Mason, A. Miller, N. Borisov, M. Antonakakis, and M. Bailey, “Outguard: Detecting In-browser Covert Cryptocurrency Mining in the Wild,” in *The World Wide Web Conference, WWW*, pp. 840–852, 2019.
- [32] H. Okhravi, M. Rabe, T. Mayberry, W. Leonard, T. Hobson, D. Bigelow, and W. Streilein, “Survey of Cyber Moving Targets,” *Massachusetts Inst of Technology Lexington Lincoln Lab, No. MIT/LL-TR-1166*, 2013.